UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/676,474	09/30/2003	Klimenty Vainstein	2222.5450000	7534

26111 7590 12/12/2007
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
PALIWAL, YOGESH	
ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
12/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/676,474	VAINSTEIN ET AL.	
	Examiner	Art Unit	
	Yogesh Paliwal	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-28 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-28 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date 10/10/2007, 10/29/2007.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

- Applicant's submission for RCE filed on October 17, 2007 has been entered.
- Applicant has amended claims 1, 14, 15, 18-24 and 26-28. Currently claims 1-28 are pending in this application.
- Examiner acknowledges clarification of claim language of claim 1 for 35 U.S.C. 101 rejections. This amendment to the claim language is determined to overcome the 35 U.S.C. 101 rejection for claims 1-13. As a result, the 35 U.S.C 101 rejection has been withdrawn for claims 1-13.

Information Disclosure Statement

1. Examiner acknowledges receiving the information disclosure statements (IDS) submitted on 10/10/2007 and 10/29/2007. Examiner also acknowledges receiving the legible copies of NPL1-NPL7, NPL10, NPL13, NPL17 (all filed with IDS submitted on 10/10/2007) and FP1-FP17, NPL1-NPL4, NPL29 and NPL31-NPL42 (all filed with IDS submitted on 10/29/2007). However examiner was not able to find the copy of NPL30 (IDS filed on 10/29/2007) reference (i.e. "Adobe Acrobat Security Settings"), as a result NPL30 has not been considered. Please provide a copy of NPL30 reference in the next correspondence.

Response to Arguments

Rejection under 35 U.S.C. 101:

- Applicant's arguments filed on 10/17/2007 regarding rejection of claims 1-13 under 35 U.S.C. 101 have been fully considered but they are not persuasive. See rejection below.

Rejection under 35 U.S.C. 102:

- Applicant's arguments with respect to claims 1-28 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

The USPTO "Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility" (Official Gazette notice of 22 November 2005), Annex IV, reads as follows:

> In contrast, a claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized, and is thus statutory. See Lowry, 32 F.3d at 1583-84, 32 USPQ2d at 1035.
>
> Claims that recite nothing but the physical characteristics of a form of energy, such as a frequency, voltage, or the strength of a magnetic field, define energy or magnetism, per se, and as such are nonstatutory natural phenomena. O'Reilly, 56 U.S. (15 How.) at 112-14. Moreover, it does not appear that a claim reciting a signal encoded with functional descriptive material falls within any of the categories of patentable subject matter set forth in Sec. 101.
>
> ... a signal does not fall within one of the four statutory classes of Sec. 101.
>
> ... signal claims are ineligible for patent protection because they do not fall within any of the four statutory classes of Sec. 101.

Claims **1-13** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter as follows. Although Claims 1-13 are directed

towards system of providing document security system, the specification provides intrinsic evidence that these claims are directed towards software alone. System as claimed in 1-13 is nothing more then software modules, which are capable of performing different tasks of the claimed system.

Note that applicant has amended claim 1 to recite an access manager module and pointed out that paragraph 112 of the instant application provides support for this limitation. However, examiner would like to point out that originally filed specification does not have 112th paragraph and examiner further believes that applicant was trying to point at paragraph 90 of the specification for the support. Paragraph 90 recites "[a]ccordingly, respective local modules in local servers, in coordination with the central server, form a distributed mechanism to provide distributed access control enforcement". However, even paragraph 90 does not provide any intrinsic evidence that access control modules are any thing other then a software program running in local servers to provide access control.

Claims 1-13 defines a system and method embodying functional descriptive material. However, the claims do not define a computer-readable medium or memory and is thus non-statutory for that reason (i.e., "When functional descriptive material is recorded on some computer-readable medium it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized" – Guidelines Annex IV). That is, the scope of the presently claimed system and method can range from paper on which the program is written, to a program simply contemplated and memorized by a

person. The examiner suggests amending the claim to embody the program on "computer-readable storage medium" or equivalent in order to make the claim statutory. Any amendment to the claim should be commensurate with its corresponding disclosure. Also note that 35 U.S.C 101 requires that claimed invention, as a whole must produce a "useful, concrete and tangible result." State Street, 149 F.3d at 1373, 47 USPQ2d at 1601-02. When the system claim list only the software part, it would not be able to produce any "useful, concrete and tangible result", in absence of corresponding hardware, as required by 35 U.S.C 101.

Examiner further would like to point out that just adding "computer-readable medium" will not be sufficient to make these claims statutory because the specification, at page 24 defines the computer readable medium as encompassing statutory media such as a "read-only memory", "random-access memory", "DC-ROMs", "DVDs", "magnetic tape", ""optical data storage devices", etc as well as ***non-statutory*** subject mater such as a "carrier waves" (which is a form of signal).

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 2, 3, 4, 5, 6, 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28 are rejected under 35 U.S.C. 102(e) as being anticipated by Leser et al. (US 2005/0028006 A1. filed as an IDS reference), hereinafter Leser.

Regarding **Claim 1**, Leser discloses a document security system for restricting access to secured documents (See Fig. 1-5) comprising:

at least one process-driven security policy that includes a plurality of states and transition rules, wherein each of the states is associated with one or more access restrictions (Fig. 1-5, and paragraphs 0096 - 0123) and wherein the transition rules specify circumstances under which a secured document is to transition from one state to another (see paragraphs 0123, 0125, two states are defined as a normal and lock-down)

an access manager module configured to determine (Paragraph 0035, "Policy Server") whether access to a secured document is permitted by a requestor based on the policy state associated therewith at the time access is requested and the corresponding one or more access restrictions thereof for the process-driven security policy (see paragraph 0035).

Regarding **Claim 2,** the rejection of claim 1 is incorporated and Leser further discloses that the one or more access restrictions for the secured document are automatically changed when the state of the process-driven security policy for the secured document changes (see paragraphs 0123 and 0125)

Regarding **Claim 3,** the rejection of claim 1 is incorporated and Leser further discloses that events cause the state of the process-driven security policy for the secured document to automatically transition from one state to another (See paragraph 0123 and 0125, "when the business process is "under attack" or otherwise vulnerable" is an event that causes switching of normal state to a "lock-down" state)

Regarding **Claim 4**, the rejection of claim 3 is incorporated and Leser further discloses that the events are internal or external events with respect to the document security system (See paragraph 0123 and 0125)

Regarding **Claim 5**, the rejection of claim 4 is incorporated and Leser further discloses that at least one of the events is an external event from a document management system (see paragraph 0123, "vulnerable to potential violations of a governmental regulation during some critical time period")

Regarding **Claim 6**, the rejection of claim 1 is incorporated and Leser further discloses that one or more of the corresponding one or more access restrictions for access to the secured document remain intact when the state of the process-driven security policy for the secured document changes (see paragraph 0123)

Regarding **Claim 8**, the rejection of claim 1 is incorporated and Leser further discloses that events cause the state of the process-driven security policy to automatically transition from one state to another (see paragraphs 0123 and 0125).

wherein the process-driven security policy includes at least a first state and a second state (see paragraph 0123, "normal" and "lock-down"), and wherein a first event causes transition from the first state to the second state (see paragraph 0123, ""under attack or otherwise vulnerable").

Regarding **Claim 9**, the rejection of claim 1 is incorporated and Leser further discloses that transition rules are based on events (see Paragraph 0123).

Regarding **Claim 11**, the rejection of claim 1 is incorporated and Leser further discloses that events cause the state of the process-driven security policy for the secured document to transition from a previous state to a current state (See Paragraph 0123), and wherein the secured document is modified when the process-driven security policy for the secured document transitions from the previous state to the current state (see paragraphs 0057, 0113, 140, 0141 and 0185).

Regarding **Claim 12**, the rejection of claim 11 is incorporated and Leser further discloses that the secured document includes at least a security information portion and an encrypted data portion (paragraph 0007, "To be effective, a rights management system must tightly couple the usage rights to the encrypted data objects so that the usage rights always appear with the associated object.") , the security information portion including at least an encrypted key, and the key being encrypted must be decrypted in order to decrypt the encrypted data portion (Paragraph 0006, "In particular,

authorized users are given access to the secret key needed to decrypt the protected object and produce the actual data object."), and wherein when the process-driven security policy for the secured document transitions from the previous state to the current state, the secured document is modified by decrypting the encrypted key and then re-encrypting the key, whereby the key is encrypted differently for the current state than the previous state (see paragraphs 0185 and 187, describing the process of re-encrypting the content encryption key (CEK) with a new Key encryption key (KEK), once the current KEK expires or need to be changed to a new KEK for any propose).

Regarding **Claim 13**, the rejection of claim 11 is incorporated and Leser further discloses when permitted, access to the secured document is available at a client machine (see paragraph 0016, "A rights-management-aware application on the end-user's machine uses the server's response to provide the end user with the owner-designated level of access to the protected segment.").

Regarding **Claims 14 and 27**, Leser discloses a method and a corresponding software program for transitioning at least one secured document through a security-policy state machine having a plurality of states, the method comprising:

(a) receiving an event (See paragraph 0123, "under attack")

(b) determining whether the event causes a state transition for the at least one secured document from a former state to a subsequent state of the security-policy state machine; (See paragraphs 0122 and 0123, describing the method of changing normal to lock-down state)

(c) automatically transitioning from the former state to the subsequent state of the security-policy state machine when determining step (b) determines that the event causes the state transition (See paragraph 0122 and 0123, "When applied to the appropriate pieces of the business process, these set of changes comprise the "lock-down" security state.")

Regarding **Claim 15**, the rejection of claim 14 is incorporated and Leser further discloses the security-policy state machine implements a process-driven security policy, and wherein each state of the security-policy state machine has different access restrictions (see Paragraph 0122, 123, Normal state allow normal processing and lock-down state lock all the access).

Regarding **Claim 16**, the rejection of claim 14 is incorporated and Leser further discloses each of the states of the security-policy state machine have different access policies (see paragraph 0122, 0123, Normal state allow normal processing and lock-down state lock all the access).

Regarding **Claim 17**, the rejection of claim 16 is incorporated and Leser further discloses the security-policy state machine is provided as part of a document security system, and wherein the different access policies of the security-policy state machine are enforced by the document security system (See, Paragraphs 0122, 0123, 0124)

Regarding **Claim 18**, the rejection of claim 14 is incorporated and Leser further discloses wherein the transitioning step (c) comprises modifying the secured document to reflect the subsequent state of the security-policy state machine (see paragraph 0185, describing the process of re-encrypting the content encryption key (CEK) with a

new Key encryption key (KEK), once the current KEK expires or need to be changed to a new KEK for any propose).

Regarding **Claim 19**, the rejection of claim 14 is incorporated and Leser further discloses the transitioning step (c) further comprising:

(c1) retrieving an encrypted file key from the secured document (Paragraph 0187, "the server 29 in step 103 decrypts the CEK using either the indicated control policy KEK or the master KEK").

(c2) decrypting, when permitted by the former state of the security-policy state machine, the encrypted file key to yield a file key (Paragraph 0187, "the server 29 in step 103 decrypts the CEK using either the indicated control policy KEK or the master KEK").

(c3) subsequently encrypting the file key in accordance with the subsequent state of the security-policy state machine (Paragraph 0187, "and re-encrypts the CEK with the current control policy KEK and master KEK"); and

(c4) storing the secured document, the secure document including at least an encrypted data portion and the subsequently encrypted file key (Paragraph 0187).

Regarding **Claim 20**, the rejection of claim 14 is incorporated and Leser further discloses that the transitioning step (c) further comprising:

(c1) retrieving an encrypted file key from the secured document; obtaining a private state key associated with the former state of the security- policy state machine (Paragraph 0187, "the server 29 in step 103 decrypts the CEK using either the indicated control policy KEK or the master KEK");

(c2) decrypting the encrypted file key using the private file key; obtaining a public state key associated with the subsequent state of the security- policy state machine (Paragraph 0187, "the server 29 in step 103 decrypts the CEK using either the indicated control policy KEK or the master KEK");

(c3) subsequently encrypting the file key in accordance with the public state key (Paragraph 0187, "and re-encrypts the CEK with the current control policy KEK and master KEK"); and

(c4) storing the secured document, the secured document including at least an encrypted data portion and the subsequently encrypted file key (Paragraph 0187).

Regarding **Claims 21 and 28**, Leser discloses a method and corresponding computer program for imposing access restrictions on electronic documents, the method comprising:

a) providing at least one process-driven security policy at a server computer, wherein the process-driven security policy is associated with a plurality of states and wherein each of the states has distinct access restriction (see paragraphs 0029, 0030 and 0096);

b) providing a reference to the process-driven security policy to client computer, the reference referring to the process-driven security policy resident on the server computer (paragraph 0039,0040 and 0073, describing the process of caching the security policies at a client computer and using then off-line).

c) associating the reference to an electronic document (Paragraph 0208, "While off-line, user A in step 144 creates a sensitive data object D (in the example, a

document) and protects it with control policy P. This action takes place while user A is disconnected from the policy server 29. Since control policy P is cached on user A's laptop, he or she is able to create and protect document D.")

d) transitioning the process-driven security policy from one state to a current state (see paragraph 0029, "Changes to a control policy would be enacted on the server storing that control policy"); and

e) subsequently determining at the server computer whether a requestor is permitted to access the electronic document, the access being based on a current state of the process-driven security policy, the current state being informed to the server computer by sending the reference to the server computer (see Paragraphs 0097 and 0035).

Regarding **Claim 22**, the rejection of claim 21 is incorporated and Leser further discloses wherein the transitioning step (d) is automatically performed based on events (Paragraph 0030).

Regarding **Claim 23**, the rejection of claim 22 is incorporated and Leser further discloses wherein the transitioning step (d) is performed at the server computer (see paragraph 0029, "Changes to a control policy would be enacted on the server storing that control policy").

Regarding **Claim 24**, the rejection of claim 21 is incorporated and Leser further discloses wherein the associating step (c) associates the reference to a group of documents (See paragraph 0097, "For example, assume that we are given a set of data objects, all of which are protected by a single control policy").

Regarding **Claim 25**, the rejection of claim 21 is incorporated and Leser further discloses wherein the method pertains to a group of electronic documents, and wherein all of the electronic documents of the group are always in the same state of the process-driven security policy (See paragraph 0097, "For example, assume that we are given a set of data objects, all of which are protected by a single control policy").

Regarding **Claim 26**, the rejection of claim 21 is incorporated and Leser further discloses evaluating the process-driven security policy of an electronic document at the server computer based on at least the security policy restrictions for the current state of the process-driven security policy for the electronic document (see Paragraphs 0097 and 0035).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Leser.

Regarding Claim 7, the rejection of claim 1 is incorporated and Leser further discloses that events cause the state of the process-driven security policy to automatically transition from one state to another (see paragraphs 0123 and 0125).

wherein the process-driven security policy includes at least a first state and a second state (see paragraph 0123, "normal" and "lock-down"), and wherein a first event

causes transition from the first state to the second state (see paragraph 0123, ""under attack or otherwise vulnerable"). However, Leser does not explicitly disclose a third state and second event that causes transition from the second state to a third state.

However Leser at paragraph 0127 recites, "Those of ordinary skill in the art should recognize the methods of extending this two-setting security knob example and implementation to one that implements an n-setting security knob, for any specific n greater then 2."

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to have a third alert state along with "normal and lock-down state", for example, a "moderate state", in which instead of going from lock-down to normal state directly, system would transit to moderate state before going to normal, in which all the people with permission to access would only be able to read the secured document and then when system would transit from moderate to normal, normal processing would be restored. The person of ordinary skill in the art would be motivated to do so because having more state provides more variations depending on the requirements of the security.

Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Leser in view of Li et al. (US 2004/0193912 A1), hereinafter Li.

Regarding **Claim 10**, the rejection of claim 9 is incorporated and Leser does not teach that the transition rules are written in XML.

However, Smith et al. in the same field of endeavor of network security discloses writing security policies in XML format (Paragraph 0014, "In one embodiment of the present invention, the security policies are stored in a relational database in a native Extensible Markup Language (XML) format")

Therefor, it would have been obvious at the time the invention was made to one of ordinary skill in the art to write the transition rules of (i.e. switching security knob rules) in XML format as taught by Li because XML is a text-based and platform independent, as a result policy server would be able to enforce and distribute the policies to all client having any type of operating system platform.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yogesh Paliwal whose telephone number is (571) 270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

YP
12/3/2007

KIM VU
PATENT EXAMI...
...GY CENTER 2100